PICO
April 1985

From Computers to Cryogenics

Stemming the Tide of Tech Transfer

by S.F. Tomajczyk

The Customs Service is involved in a number of lengthy and complicated investigations into conspiracies which, when they become public knowledge, will shake the high-technology industry to its roots. Make no mistake. Our investigators have uncovered wide gaps in America's ability to keep our technology safe from our adversaries.

William von Raab,
U.S. Commissioner of Customs

The chief executive officer of a small computer firm located outside Boston happens to overhear a conversation between the company's order processor and a friend during lunch.

"It's weird," mentions the order processor, sipping a Coke and fingering a half-eaten sandwich. "Who'd ever in their right mind want to have their expansion boards special-packaged with plastic bubble sheets and silica? I mean, sure, if it were going overseas to Europe or something I'd understand—but New York? It's just five hours from here. They're just wasting their money."

He laughs. "Oh well, guess I shouldn't complain too much. After all, I don't have to do the shipping, and besides, the extra bucks that company is paying will end up in my pocket at the end of the year as a bonus check." He bites into his sandwich while his friend nods silently in agreement.

The CEO gets up abruptly and marches back to his office. Flipping through his Rolodex, he finally finds the number he's looking for and dials it quickly.

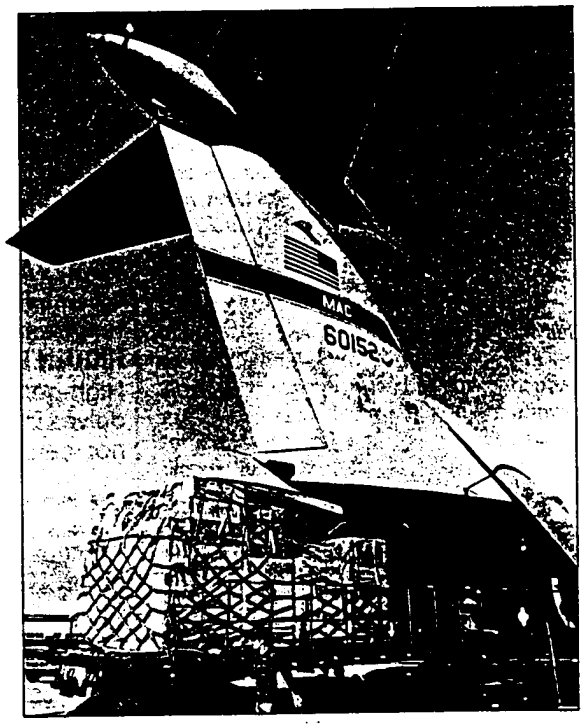
Meanwhile, in Washington, D.C., in a "secured" room on the sixth floor of the U.S. Customs Service building, a phone rings. A special agent, revolver on hip, leans across one of the many computer terminals and answers the phone. "Operation Exodus Command Center, may I help you?"

Thus begins the pulling of the plug on technology transfer. The Exodus Command Center sends U.S. Customs agents from the Boston field office to visit the computer firm and exchange the contents of the expansion board shipment with 52 pounds of "Love Me Tender" dog food. Agents then monitor the shipment carefully and trace it throughout its journey to New York.

After days of constant surveillance, U.S. Customs agents finally arrest the "high-tech smuggler" at New York Harbor just eight minutes before a ship destined for Malmo, Sweden, embarks with the so-called "New York-bound" cargo. Both the dog food and the computer components are safe. American technology has again been rescued from one of many high-tech pipelines to the Kremlin.

Scenarios such as the one above are not unusual. Indeed, they occur much more often than most people would like to believe. Technology transfer, or the illegal export of American high-technology know-how, equipment and strategic material to the USSR and the other nations of the Soviet bloc is a very serious matter in today's high-tech-oriented world. Our national security rests upon our ability to stem the flow of information and equipment to other countries.

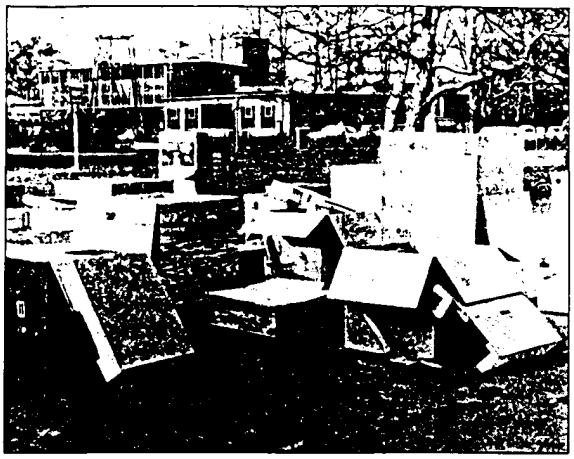
Technology transfer is not new. It's been around since some caveman first discovered fire and someone else wanted it without having to go through all the trial and error. But the dangers and implications of tech transfer have been magnified significantly since World War II when high technology was born in the research and



Computer equipment seized by West Germany on behalf of U.S. Customs is unloaded after it was returned to Andrews Air Force Base, Maryland, aboard a C-141 military cargo plane. The sensitive cargo was escorted back to the United States by a Special Agent assigned to the U.S. Customs Attache in Bonn, West Germany. Courtesy of U.S. Department of Defense.

S.F. Tomajczyk is a New Hampshire-based freelance writer whose work has appeared in Yankee, Writer's Digest, Metropolitan Detroit, *and a number of other magazines.* *The author would like to thank the following individuals and agencies for their time and information while he was conducting the research for this article: Dr. Stephen D. Bryen, Deputy Assistant Secretary of Defense; Betty Sprigg, Deputy Chief, Department of Defense; Barbara Ledeen, Counselor, Department of Defense; Chris Frazier, U.S. Customs; Roger Urbanski, Director, U.S. Customs Strategic Investigative Division; Gary Waugh, Chief of U.S. Customs Technology Branch; Senior Special Agent Ed Bryant, U.S. Customs; William Meehan, Chief of Exodus Command Center; the Department of Commerce; the Garn Committee, U.S. Senate; the Office of East-West Trade, Department of State; Ernie Porter, Federal Bureau of Investigation; and computer security consultant Edward F. Sayle.*

Continued



Approximately 10 tons of militarily critical computer technology about to be diverted to the Soviet Union were seized recently in Germany in a joint U.S./German Customs action. Identifying markings on the outside of many of the shipping containers were obliterated. Photo: Courtesy of U.S. Department of Defense.

development laboratory. And in those subsequent 40 years, the Warsaw Pact nations and their allies have acquired a vast amount of U.S. and Western technology—especially in the computer field.

Pipelines to Russia

"The Soviets' number one priority," remarks Gary Waugh, chief of the U.S. Customs Technology Branch, "is to overcome a 10-year Western lead in computer technology. And they'll do just about anything in order to accomplish that goal."

Each year, after the Soviet government and scientific community have identified their technological needs, detailed "shopping lists" are distributed to thousands of Soviet diplomats, scientists, business professionals, students and spies. (Note that in 1983, more than 17,000 Soviet-bloc scholars, tourists and diplomats entered the United States.) They do whatever it takes to obtain secrets, beginning with purchase, and extending to bribery, blackmail, theft, and even searching trash bins.

Their task is not as difficult as it might sound. An amazing amount of technological information can be obtained *legally* through several U.S. government agencies, including the National Aeronautics and Space Administration, General Services Administration, Government Printing Office and National Technology Information Service. Anything that has been paid for by tax dollars—White House floor plans, detailed information concerning Soviet and American military forces, blueprints of the Space Shuttle—must be made available to the general public, and is thereby accessible to the Russians. It appears that America's greatest strength—an open flow of information—may also be its greatest potential weakness.

Once the desired material is secured, it is then smuggled out of the U.S. through Canada, Mexico or Europe. In some cases, computer documents and equipment are even transferred via Soviet vessels waiting offshore, or within sacrosanct diplomatic pouches.

Although such clandestine activities would prove dangerous and embarrassing to the Soviets if they were caught red-handed, these operations are nonetheless quite beneficial in the long run. Technology transfer reduces the Soviets' research and development risk, reduces time and cost, enhances their technological base, results in faster deployment of countermeasures to our systems, and increases their supply of advanced-weapon sales to Eastern-bloc nations.

Senator Sam Nunn (D) of Georgia agrees that the danger facing us is significant. "The Soviets have come to view our technology as *their* technology, to be obtained whenever they want it," he remarks. "As a consequence, we are in the position of supporting our own costly national security apparatus and indirectly helping them to build theirs."

A few recent examples demonstrate how America might have helped Russia leapfrog the 10-year computer gap if these activities had not been detected and stopped:

*Five men were indicted and accused of establishing a firm in California to send computer equipment to Bulgaria, a close Soviet ally. The computer parts were shipped via a front company in the Netherlands.

*An American computer executive was offered almost a half-million dollars by the Soviet Union, to be deposited in a Swiss bank account, in return for the source code to a computer program with military potential.

*Customs agents impounded a $1.5 million computer shipment in Halsingborg, Sweden, bound for the Soviet Union. The shipment included a VAX 11/782 minicomputer capable of performing missile guidance and global monitoring of military operations.

*U.S. Customs and FBI special agents seized electronic equipment that had been purchased by a member of the Cuban delegation to the United Nations. The diplomat had obtained the material from a Florida company by mail. Federal agents seized the equipment before it was shipped via UPS to the Cuban mission in New York.

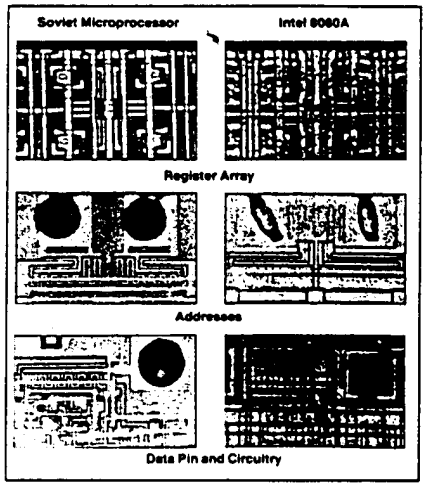
With the Soviets launching this determined, sustained attack on the security of our computer technology, what steps is America taking to retaliate and prevent what the Reagan administration once referred to as a "massive hemorrhage?" Surely the U.S. government must be doing something?

Yes, federal agencies are engaged in an all-out effort to block the pipelines.

Damming the Flow

The Department of Commerce administers and revises a list (called the Critical Control List or CCL) of some 200,000 items that cannot be exported to Eastern-bloc countries. In addition, the Department of Defense monitors its own 700-page listing of non-exportable military products and technologies—the MCTL—through its internal Technology Transfer Control Program. The material that eventually goes on the CCL, and sometimes the MCTL, is determined by several committees, among which the multilateral Coordinating Committee for Export Controls (CoCom) plays a major role.

CoCom's 15-nation membership (Japan plus all NATO countries except Iceland and Spain) meets every Tuesday in Paris to discuss, update and establish guidelines for products and technologies that should be controlled. In addition, CoCom representatives review requests and vote on granting permission to ship embargoed items to a



Under the microscope, similarities between Soviet and US microprocessors become too close for coincidence.

Continued

member nation. And, perhaps more importantly, CoCom members also unite their enforcement agencies to stop unlawful exports passing through their nations on the way to Russia and Soviet-bloc countries.

Currently, controls on computers, especially picos, established by CoCom, are extremely rigid. Exports must be on a government-to-government basis, and the list of "friendly" governments is short. Countries in which intermediaries would be likely to obtain U.S. computers, such as Hong Kong, Switzerland and England, have a difficult time importing such technology from America. "We want to try to keep the East behind, we don't want them ahead of us," remarks a spokesman from the Office of East-West Trade at the Department of State. "We're trying to squeeze Russia's throat a little bit."

The exportability of most computers is determined by a performance parameter. The data processing rate (DPR) is the most common criterion: the faster a computer is, the less chance it has for exportation. Picos, however, follow the beat of a different drummer. In a report to Congress in February 1984, Secretary of Defense Caspar W. Weinberger stressed the need for new and tighter multilateral controls for picos, primarily because their "small size, weight, power and rugged packaging have high military utility."

Today, any pico or microcomputer that is "ruggedized," tempest-treated (shielded with metal to prevent the emission of radio waves, see "The Covert Computer" in last month's *PICO* for more information), has a DPR over 48 bits per second, is capable of being upgraded to achieve compatibility with Soviet bloc-manufactured systems, has a large bubble memory, or is capable of microelectronic manufacturing or design (CAD/CAM, for example) is prohibited for export. This definition includes the Grid Compass, Hewlett-Packard 110 and the now defunct Gavilan computer company's picocomputers.

The U.S. Customs Service is the governmental arm that ensures prohibited technology and equipment are not exported to Soviet-bloc nations. In addition to overseeing more than 400 provisions of the law on behalf of some 40 other federal agencies, U.S. Customs also enforces both the Export Administration Act of 1979 and the Arms Export Control Act of 1976 through "Operation Exodus."

Launched in October 1981 with just four agents, Operation Exodus has grown to require an integrated national staff of several hundred inspectors, special agents and other officers. In addtion, its liaison officers in allied countries cooperate with their governments in preventing and seizing illegal exports bound for Russia. A top-security Command Center in Washington, D.C. (the door to which is guarded by three locks, including a code-button device), monitors and supports the various operations conducted by task forces around the world.

The Exodus program is designed to prevent technology transfer, not to restrict or discourage legitimate U.S. export. In fact, Exodus agents visit potential tech-transfer victims, such as computer and semiconductor manfacturers, to show them how to detect illegal export and how to apply properly for export licenses. Knowledge is Operation Exodus' greatest strength.

Gary Mayer, chief of U.S. Customs Technology, says firmly, "Yes, we're making an impact on illegal export. We've put up hurdles in their paths, forcing them to spend more money and take greater chances.

"There seems to be a certain parallel between it and narcotics smuggling. One way that you can tell if you're making an impact on narcotics smuggling is when the price on the street goes up.

"Likewise, we're making an impact with Exodus," Mayer claims. "We've obviously made it more difficult for these people, because they've changed their routes and are forced to do things that aren't very cost-effective. Our seizure-to-detention rate is good, about 61 percent, which means we're getting more accurate in our searches. *That* tends to put a bit of fear into your average smuggler's heart."

Exodus' report card for the past four years further substantiates this news. As of October 1984, Operation Exodus has seized more than 3,700 shipments of high-tech equipment worth in excess of $226 million, and more than 434 arrests have been made, resulting in 588 indictments and 350 convictions. According to Senior Special Agent Ed Bryant, businesses have also become more aware of proper licensing.

"Our statistics pretty much speak for themselves," he says. "Back in 1981 there were perhaps 50,000 individual validated export licenses applied for with the Department of Commerce. Today it's at least 120,000, which demonstrates that there were 70,000 shipments that were going without a license before, but that are now being licensed."

U.S. Customs has produced a progress report of which any parent would be proud.

The Dripping Faucet

Unfortunately, technology transfer is a long way from extinction. Granted, the pipelines to the Kremlin are becoming clogged with debris, thank to CoCom, Exodus, the FBI and other agencies, but the constant dripping of tech-transfer will always be around.

For example, a Soviet spy can easily walk into Toys 'R' Us or any similar store and buy a toy that has a microprocessor in it. The agent returns to his hotel room, tears the toy apart, pulls out the chip, and checks off a box on his "shopping list."

While our military systems are typically five years behind state-of-the-art technology because of lengthy testing procedures, commercial toys are not. Manufacturers know that state-of-the-art sells, so that's what goes into their products, whether or not all the bugs have been worked out. The Russians will find uses for that "toy" in military and nonmilitary designs long before the same chip is finally incorporated into similar American applications. But in the complex world of technology transfer, shutting off the trickle of information to the East is no child's game. ■

Continued

How Do You Spot a Spy?

by S.F. Tomajczyk

While the U.S. Customs Service spot-checks hundreds of outgoing shipments around the nation each day for illegal export of American technology, it is important the private business sector also be aware of how to identify technology transfer in progress.

"Once you lose the technology, you lose your advantage forever," remarks counselor Barbara Ledeen, Department of Defense. "It's important that businesses inform the government of suspicious activities because if someone is indeed sacrificing our national security for their own gain, it must be put to an immediate halt. Cooperation from the private business sector is necessary and welcomed."

Just how do you detect a Russian spy at work?

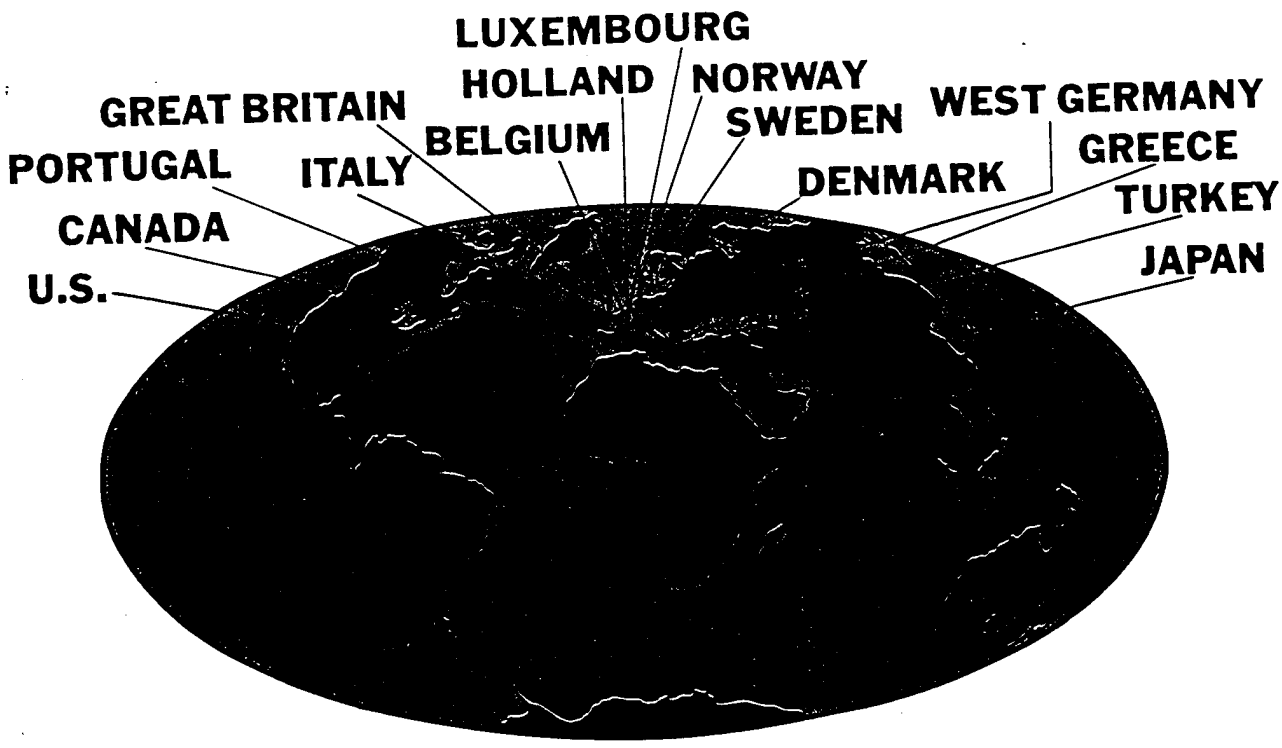
"Well, for the most part," says Senior Special Agent Ed Bryant, U.S. Customs, you'd probably never recognize a Soviet agent. They're truly professional. They warm up to you at a business meeting, and then try to convince you to help them.

"Once you lose the technology, you lose your advantage forever."

They're intelligent and easy to get along with—it's just about impossible to spot an agent right off the bat. Even seasoned professional agents are never certain.

So much for seeing beneath the cloak-and-dagger of a Russian spy or smuggler. But don't give up—the following is a list of warning signals from Operation Exodus that should help you detect possible export violations.

1. Orders from little-known customers with no obvious use for the items or quantities involved or no suitable facilities in which to use them, or customers who refuse to identify end users.
2. Inquiries and orders with one or more of the following characteristics may indicate a foreign destination, even though purported to be domestic sales:
   a. specifications of 230v/50hz, 115v/50hz, or unusual power cords, fuses or powerlines.
   b. requests for illogical options or merchandise.
   c. instructions for special salt spray or



The 15 nations of the Coordinating Committee for Export Controls (CoCom) determine the products and technologies its members are forbidden to export to Soviet-bloc countries.

Continued

humidity, packing, and/or export marking.

...instructions to make direct shipments to trading companies, freight forwarders or export companies.

...circuitous routing (computing that is economically illogical, particularly through Canada to a non-Canadian end-user).

...domestic delivery instructions to companies with no apparent connection to the purchaser.

...requests for cubic volumes and/or packaged weights, especially in metric tons.

...certification as to country of origin or conformance to international standards.

...specifying terms of payment involving drafts drawn on foreign banks or other special banking requirements.

...requests for exemption from state tax with an unwillingness to provide state resale identification numbers.

...orders placed by firms or individuals other than the end-user, from foreign countries.

...unusual behavior by customers and unusual or extremely lucrative financial compensation for merchandise to be purchased.

If you suspect either technology transfer or an export violation at your place of work, or if you have questions concerning licensing regulations, contact the appropriate agency listed below. Except where noted, usual hours of operation are Monday through Friday, 8 a.m. to 5 p.m.

Operation Exodus Command Center
Customs Operations and Suspicious Activity Reporting
(202) 566-9464 (24-hour line, *emergencies only* after 5 p.m.)

U.S. Customs Service
Office of Enforcement
1301 Constitution Ave. N.W.
Washington, D.C. 20229

Department of Commerce
Licensing and Export Regulation
(202) 377-4811

Department of Commerce
Export Enforcement
Los Angeles (213) 536-6911
District of Columbia (202) 377-4608
San Francisco (415) 876-9292
New York (212) 264-1365

Department of Defense
Industry/Government Liason Office
(cases in progress and information on technical security)
(202) 697-7840

If you would like to learn more about technology transfer and industrial espionage, suggested reading material includes *Industrial Espionage, Intelligence Techniques and Countermeasures* by Norman R. Bottom Jr. and Robert J. Galati (Butterworth Publishers, Stoneham, MA, 1984, $24.95) and *Industrial Intelligence and Espionage* by Paul I. Slee Smith (London, 1970). ■

Microelectronic Equipment and Technology Legally and Illegally Acquired by the Soviet Bloc

Equipment or Technology	Comments
Process Technology for Microelectronic Wafer Preparation	The Soviets have acquired hundreds of specific pieces of equipment related to wafer preparation, including expitaxial growth furnaces, crystal pullers, rinsers/dryers, slicers, and lapping and polishing units.
Process Technology for Producing Circuit Masks	Many acquisitions in this area include computer-aided design software, pattern generators and compilers, digital plotters, photorepeaters, contact printers, mask comparators, electron-beam generators, and ion milling equipment.
Equipment for Device Fabrication	Many hundreds of acquisitions in this area have provided the Soviets with mask aligners, diffusion furnaces, ion implanters, coaters, etchers, and photochemical process lines.
Assembly and Test Equipment	Hundreds of items of Western equipment, including scribers, bonders, probe testers, and final test equipment have been acquired by the Soviets.

Major Fields of Technology of Interest to Soviet and East European Visitors to the United States

Computers	Architecture	Memories
	Automatic Control	N/C (Numerically Controlled) Units
	CAD (Computer-Aided Design)	Networks
	Cybernetics/Artificial Intelligence	Pattern Recognition
	Data Bases	Programming
	Image Processing Design	Robots
	Image Processing/Retrieval	Software
Materials	Amorphous	Metallurgy
	CAD	N/C Machine Tools
	Composites	Powder Metals
	Cryogenics	Superconductors
	Deformation	Testing/NDT (Non-Destructive)
Semiconductors	CAD	Design
	Circuits	Ion Implantation
	Defects	Production Technology
	Devices	SAW (Surface Acoustic Wave) Devices
Communications, Navigation, and Control	Antennas	Satellite Communications
	Microwave/Millimeter Waves	Signal Processing
	Radio Wave Propagation	Telecommunications
Vehicular/Transportation	Marine Systems	Shipbuilding
Laser and Optics	Fiber Optics	Optics
	Gas Lasers	Tunable Lasers
Nuclear Physics	Cryogenics	Reactors
	Fusion	Structural Designs
	Materials	Superconductors
	MHD (Magnetohydrodynamics)	
Microbiology	Genetic Engineering	